AMENDMENTS TO THE CLAIMS:

This listing of claims will replace all prior versions and listings of claims in the application:

1. (Currently Amended) A method for issuing a digital certificate for a user on a network, comprising the steps of:

linking a physical address of a user to an electronic account of the user and thereby enabling the user to receive information sent to the electronic account at the physical address or enabling the user to receive information sent to the physical address in the electronic account;

receiving a request for a digital certificate for ~~a~~ the user having ~~an~~ the electronic account~~, wherein the electronic account is linked to a physical address of the user~~;

generating~~, by a certificate authority,~~ the digital certificate for the user, wherein the digital certificate includes information enabling authentication of a transaction on the network; and

linking the digital certificate to the electronic account of the user.

2. (Original) The method of claim 1, further comprising the step of:

storing a reference to the digital certificate in a certificate directory at the certificate authority.

3. (Original) The method of claim 1, wherein the certificate authority includes a proofing server.

4. (Original) The method of claim 3, wherein the certificate authority further includes a proofing workstation.

5. (Original) The method of claim 1, wherein the certificate authority is a United States Postal Service digital certificate authority.

6. (Original) The method of claim 1, wherein the digital certificate includes an identifier of the user.

7. (Original) The method of claim 1, wherein the digital certificate includes a certificate serial number.

8. (Original) The method of claim 1, wherein the digital certificate includes a certificate validity period.

9. (Original) The method of claim 1, wherein the digital certificate includes a proofing workstation validation.

10. (Original) The method of claim 1, wherein the digital certificate includes a public key for authenticating the digital certificate.

11. (Original) The method of claim 1, wherein the digital certificate includes an identifier of the certificate authority.

12. (Original) The method of claim 1, wherein the digital certificate includes a certificate status.

13. (Original) The method of claim 12, wherein the certificate status is set to active.

14. (Original) The method of claim 12, wherein the certificate status is set to hold.

15. (Original) The method of claim 12, wherein the certificate status is set to revoked.

16. (Currently Amended) A method for issuing a digital certificate for a user on a network, comprising the steps of:

receiving, at a proofing server, a request for a digital certificate from a user with an electronic account, wherein the electronic account is linked to a physical address of the user to thereby enable the user to receive information sent to the electronic account at the physical address or to thereby enable the user to receive information sent to the physical address in the electronic account;

generating, by the proofing server, the digital certificate for the user;

setting a status of the digital certificate to hold, by the proofing server;

sending the request for the digital certificate to a proofing workstation;

verifying, at the proofing workstation, the identity of the user;

sending an identification verification from the proofing workstation to the proofing server, when the identity of the user is verified;

setting the status of the digital certificate to active in response to the identification verification; and

storing the digital certificate in the electronic account of the user.

17. (Original) The method of claim 16, further comprising the step of:

linking the digital certificate to a transaction on the network by the user, wherein the digital certificate can be used to authenticate the transaction.

18. (Original) The method of claim 16, further comprising the step of:

storing a reference to the digital certificate in a certificate directory at the proofing server.

19. (Original) The method of claim 16, further comprising the step of:

setting the status of the digital certificate to revoked.

20. (Original) The method of claim 19, further comprising the step of:

storing a reference to the digital certificate in a certificate revocation list at the proofing server.

21. (Original) The method of claim 16, further comprising the step of:

sending a private key from the proofing workstation to the proofing server, when the identity of the user is verified.

22. (Original) The method of claim 21, further comprising the step of:

verifying the private key, by the proofing server, before setting the status of the digital certificate to active.

23. (Original) The method of claim 16, wherein the proofing workstation includes a bar code scanner.

24. (Original) The method of claim 23, wherein the identification verification is a bar code.

25. (Original) The method of claim 16, wherein the proofing workstation includes a credit card reader.

26. (Original) The method of claim 16, wherein the proofing workstation includes a smart card interface.

27. (Original) The method of claim 16, wherein the proofing server is a United States Postal Service proofing server.

28. (Original) The method of claim 16, wherein the proofing workstation is a United States Postal Service proofing workstation.

29. (Currently Amended) A method for processing a request for a digital certificate from a user, comprising the steps of:

receiving, at a proofing workstation, user information for a user with an electronic account, wherein the electronic account is linked to a physical address of the user to thereby enable the user to receive information sent to the electronic account at the physical address or to thereby enable the user to receive information sent to the physical address in the electronic account;

receiving identification information from the user at the proofing workstation;

matching the user information to the identification information by the proofing workstation; and

sending an identification verification from the proofing workstation to a proofing server, when the user information has been matched to the identification information.

30. (Original) The method of claim 29, further comprising the step of :

receiving payment from the user at the proofing workstation.

31. (Original) The method of claim 30, wherein the payment is received via credit card.

32. (Original) The method of claim 30, wherein the payment is received via Smart Card.

33. (Original) The method of claim 29, wherein the proofing workstation includes a bar code reader.

34. (Original) The method of claim 33, wherein the identification verification is a bar code.

35. (Original) The method of claim 29, wherein the proofing workstation is a United States Postal Service proofing workstation.

36. (Currently Amended) A method for issuing a digital certificate for a user on a network, comprising the steps of:

receiving, at a proofing server, a request for a digital certificate from a user with an electronic account, wherein the electronic account is linked to a physical address of the user to thereby enable the user to receive information sent to the electronic account at the physical address or to thereby enable the user to receive information sent to the physical address in the electronic account, and wherein the request includes user information;

sending the user information to a proofing workstation via the network;

generating, by the proofing server, the digital certificate for the user;

setting a status of the digital certificate to hold, by the proofing server;

receiving an identification verification from the proofing workstation when the identity of the user has been verified by the proofing workstation;

setting the status of the digital certificate to active in response to the identification verification; and

storing the digital certificate in the electronic account of the user.

37. (Original) The method of claim 36, further comprising the step of:

storing a reference to the digital certificate in a certificate directory at the proofing server.

38. (Original) The method of claim 36, further comprising the step of:

setting the status of the digital certificate to revoked.

39. (Original) The method of claim 38, further comprising the step of:

storing a reference to the digital certificate in a certificate revocation list at the proofing server.

40. (Original) The method of claim 36, further comprising the step of:

receiving a private key from the proofing workstation, when the identity of the user is verified.

41. (Original) The method of claim 40, further comprising the step of:

verifying the private key before setting the status of the digital certificate to active.

42. (Original) The method of claim 36, wherein the proofing server is a United States Postal Service proofing server.

43. (Currently Amended) A system for issuing a digital certificate for a user on a network, comprising:

a receiving component configured to receive a request for a digital certificate for a user having an electronic account, wherein the electronic account is linked to a physical address of the user to thereby enable the user to receive information sent to the electronic account at the physical address or to thereby enable the user to receive information sent to the physical address in the electronic account;

a generating component configured to generate the digital certificate for the user, wherein the digital certificate includes information enabling authentication of a transaction on the network; and

a linking component configured to link the digital certificate to the electronic account of the user.

44. (Original) The system of claim 43, further comprising:

a storing component configured to store a reference to the digital certificate in a certificate directory at the generating component.

45. (Original) The system of claim 43, wherein the generating component includes a proofing server.

46. (Original) The system of claim 45, wherein the generating component further includes a proofing workstation.

47. (Original) The system of claim 43, wherein the generating component is a United States Postal Service digital certificate authority.

48. (Original) The system of claim 43, wherein the digital certificate includes an identifier of the user.

49. (Original) The system of claim 43, wherein the digital certificate includes a certificate serial number.

50. (Original) The system of claim 43, wherein the digital certificate includes a certificate validity period.

51. (Original) The system of claim 43, wherein the digital certificate includes a proofing workstation validation.

52. (Original) The system of claim 43, wherein the digital certificate includes a public key for authenticating the digital certificate.

53. (Original) The system of claim 43, wherein the digital certificate includes an identifier of the certificate authority.

54. (Original) The system of claim 43, wherein the digital certificate includes a certificate status.

55. (Original) The system of claim 54, wherein the certificate status is set to active.

56. (Original) The system of claim 54, wherein the certificate status is set to hold.

57. (Original) The system of claim 54, wherein the certificate status is set to revoked.

58. (Currently Amended) A system for issuing a digital certificate for a user on a network, comprising:

a receiving component configured to receive a request for a digital certificate from a user with an electronic account, wherein the electronic account is linked to a physical address of the user to thereby enable the user to receive information sent to the electronic account at the physical address or to thereby enable the user to receive information sent to the physical address in the electronic account;

a generating component configured to generate the digital certificate for the user;

a hold setting component configured to set a status of the digital certificate to hold, by the proofing server;

a request sending component configured to send the request for the digital certificate to a proofing workstation;

a verifying component configured to verify the identity of the user;

a verification sending component configured to send an identification verification from the proofing workstation to the proofing server, when the identity of the user is verified;

an active setting component configured to set the status of the digital certificate to active in response to the identification verification; and

a storing component configured to store the digital certificate in the electronic account of the user.

59. (Original) The system of claim 58, further comprising:

a linking component configured to link the digital certificate to a transaction on the network by the user, wherein the digital certificate can be used to authenticate the transaction.

60. (Original) The system of claim 58, further comprising:

a reference storing component configured to store a reference to the digital certificate in a certificate directory at the proofing server.

61. (Original) The system of claim 58, further comprising:

a revoked setting component configured to set the status of the digital certificate to revoked.

62. (Original) The system of claim 61, further comprising:

a revoked storing component configured to store a reference to the digital certificate in a certificate revocation list at the proofing server.

63. (Original) The system of claim 58, further comprising:

a key sending component configured to send a private key from the proofing workstation to the proofing server, when the identity of the user is verified.

64. (Original) The system of claim 63, further comprising:

a key verifying component configured to verify the private key before setting the status of the digital certificate to active.

65. (Original) The system of claim 58, wherein the proofing workstation includes a bar code scanner.

66. (Original) The system of claim 65, wherein the identification verification is a bar code.

67. (Original) The system of claim 58, wherein the proofing workstation includes a credit card reader.

68. (Original) The system of claim 58, wherein the proofing workstation includes a smart card interface.

69. (Original) The system of claim 58, wherein the proofing server is a United States Postal Service proofing server.

70. (Original) The system of claim 58, wherein the proofing workstation is a United States Postal Service proofing workstation.

71. (Currently Amended) A system for processing a request for a digital certificate from a user, comprising:

a user information receiving component configured to receive user information for a user with an electronic account, wherein the electronic account is linked to a physical address of the user to thereby enable the user to receive information sent to the electronic account at the physical address or to thereby enable the user to receive information sent to the physical address in the electronic account;

an identification receiving component configured to receive identification information from the user at the proofing workstation;

a matching component configured to match the user information to the identification information by the proofing workstation; and

a verification sending component configured to send an identification verification from the proofing workstation to a proofing server, when the user information has been matched to the identification information.

72. (Original) The system of claim 71, further comprising:

a payment receiving component configured to receive payment from the user at the proofing workstation.

73. (Original) The system of claim 72, wherein the payment is received via credit card.

74. (Original) The system of claim 72, wherein the payment is received via Smart Card.

75. (Original) The system of claim 71, wherein the proofing workstation includes a bar code reader.

76. (Original) The system of claim 75, wherein the identification verification is a bar code.

77. (Original) The system of claim 71, wherein the proofing workstation is a United States Postal Service proofing workstation.

78. (Currently Amended) A system for issuing a digital certificate for a user on a network, comprising:

a request receiving component configured to receive a request for a digital certificate from a user with an electronic account, wherein the electronic account is linked to a physical address of the user to thereby enable the user to receive information sent to the electronic account at the physical address or to thereby enable

the user to receive information sent to the physical address in the electronic account, and wherein the request includes user information;

a user information sending component configured to send the user information to a proofing workstation via the network;

a certificate receiving component configured to receive the digital certificate for the user;

a hold setting component configured to set a status of the digital certificate to hold, by the proofing server;

a verification receiving component configured to receive an identification verification from the proofing workstation when the identity of the user has been verified by the proofing workstation;

an active setting component configured to set the status of the digital certificate to active in response to the identification verification; and

a storing component configured to store the digital certificate in the electronic account of the user.

79. (Original) The system of claim 78, further comprising:

a reference storing component configured to store a reference to the digital certificate in a certificate directory at the proofing server.

80. (Original) The system of claim 78, further comprising:

a revoked setting component configured to set the status of the digital certificate to revoked.

81. (Original) The system of claim 80, further comprising:

a revoked storing component configured to store a reference to the digital certificate in a certificate revocation list at the proofing server.

82. (Original) The system of claim 78, further comprising:

a key receiving component configured to receive a private key from the proofing workstation, when the identity of the user is verified.

83. (Original) The system of claim 82, further comprising:

a key verifying component configured to verify the private key before setting the status of the digital certificate to active.

84. (Original) The system of claim 78, wherein the proofing server is a United States Postal Service proofing server.

85. (Currently Amended) A computer readable medium having computer readable code embodied therein for issuing a digital certificate for a user on a network, the computer readable code comprising:

a receiving module configured to receive a request for a digital certificate for a user having an electronic account, wherein the electronic account is linked to a physical address of the user to thereby enable the user to receive information sent to the electronic account at the physical address or to thereby enable the user to receive information sent to the physical address in the electronic account;

a generating module configured to generate the digital certificate for the user, wherein the digital certificate includes information enabling authentication of a transaction on the network; and

a linking module configured to link the digital certificate to the electronic account of the user.

86. (Currently Amended) A computer readable medium having computer readable code embodied therein for issuing a digital certificate for a user on a network, the computer readable code comprising:

a request receiving module configured to receive a request for a digital certificate from a user with an electronic account, wherein the electronic account is linked to a physical address of the user to thereby enable the user to receive information sent to the electronic account at the physical address or to thereby enable the user to receive information sent to the physical address in the electronic account;

a generating module configured to generate the digital certificate for the user;

a hold setting module configured to set a status of the digital certificate to hold, by the proofing server;

a request sending module configured to send the request for the digital certificate to a proofing workstation;

an identity verifying module configured to verify the identity of the user;

a verification sending module configured to send an identification verification from the proofing workstation to the proofing server, when the identity of the user is verified;

an active setting module configured to set the status of the digital certificate to active in response to the identification verification; and

a storing module configured to store the digital certificate in the electronic account of the user.

87. (Currently Amended) A computer readable medium having computer readable code embodied therein for processing a request for a digital certificate from a user, the computer readable code comprising:

an information receiving module configured to receive user information for a user with an electronic account, wherein the electronic account is linked to a physical address of the user to thereby enable the user to receive information sent to the electronic account at the physical address or to thereby enable the user to receive information sent to the physical address in the electronic account;

an identification receiving module configured to receive identification information from the user at the proofing workstation;

a matching module configured to match the user information to the identification information by the proofing workstation; and

a sending module configured to send an identification verification from the proofing workstation to a proofing server, when the user information has been matched to the identification information.

88. (Currently Amended) A computer readable medium having computer readable code embodied therein for issuing a digital certificate for a user on a network, the computer readable code comprising:

a request receiving module configured to receive a request for a digital certificate from a user with an electronic account, wherein the electronic account is linked to a physical address of the user to thereby enable the user to receive information sent to the electronic account at the physical address or to thereby enable the user to receive

information sent to the physical address in the electronic account, and wherein the request includes user information;

a sending module configured to send the user information to a proofing workstation via the network;

a generating module configured to generate the digital certificate for the user;

a hold setting module configured to set a status of the digital certificate to hold, by the proofing server;

a verification receiving module configured to receive an identification verification from the proofing workstation when the identity of the user has been verified by the proofing workstation;

an active setting module configured to set the status of the digital certificate to active in response to the identification verification; and

a storing module configured to store the digital certificate in the electronic account of the user.

89. (Currently Amended) A system for issuing a digital certificate for a user on a network, comprising:

means for receiving a request for a digital certificate for a user having an electronic account, wherein the electronic account is linked to a physical address of the user to thereby enable the user to receive information sent to the electronic account at the physical address or to thereby enable the user to receive information sent to the physical address in the electronic account;

means for generating, by a certificate authority, the digital certificate for the user, wherein the digital certificate includes information enabling authentication of a transaction on the network; and

means for linking the digital certificate to the electronic account of the user.

90. (Currently Amended) A system for issuing a digital certificate for a user on a network, comprising:

means for receiving, at a proofing server, a request for a digital certificate from a user with an electronic account, wherein the electronic account is linked to a physical address of the user to thereby enable the user to receive information sent to the electronic account at the physical address or to thereby enable the user to receive information sent to the physical address in the electronic account;

means for generating, by the proofing server, the digital certificate for the user;

means for setting a status of the digital certificate to hold, by the proofing server;

means for sending the request for the digital certificate to a proofing workstation;

means for verifying, at the proofing workstation, the identity of the user;

means for sending an identification verification from the proofing workstation to the proofing server, when the identity of the user is verified;

means for setting the status of the digital certificate to active in response to the identification verification; and

means for storing the digital certificate in the electronic account of the user.

91. (Currently Amended) A system for processing a request for a digital certificate from a user, comprising:

means for receiving, at a proofing workstation, user information for a user with an electronic account, wherein the electronic account is linked to a physical address of the user to thereby enable the user to receive information sent to the electronic account at the physical address or to thereby enable the user to receive information sent to the physical address in the electronic account;

means for receiving identification information from the user at the proofing workstation;

means for matching the user information to the identification information by the proofing workstation; and

means for sending an identification verification from the proofing workstation to a proofing server, when the user information has been matched to the identification information.

92. (Currently Amended) A system for issuing a digital certificate for a user on a network, comprising:

means for receiving, at a proofing server, a request for a digital certificate from a user with an electronic account, wherein the electronic account is linked to a physical address of the user to thereby enable the user to receive information sent to the electronic account at the physical address or to thereby enable the user to receive information sent to the physical address in the electronic account, and wherein the request includes user information;

means for sending the user information to a proofing workstation via the network;

means for generating, by the proofing server, the digital certificate for the user;

means for setting a status of the digital certificate to hold, by the proofing server;

means for receiving an identification verification from the proofing workstation when the identity of the user has been verified by the proofing workstation;

means for setting the status of the digital certificate to active in response to the identification verification; and

means for storing the digital certificate in the electronic account of the user.